

Randall E. Kay (State Bar No. 149369)
rekay@jonesday.com
JONES DAY
4655 Executive Drive, Suite 1500
San Diego, CA 92121.3134
Telephone: +1.858.314.1200
Facsimile: +1.844.345.3178

Marcus S. Quintanilla (State Bar No. 205994)
mquintanilla@jonesday.com
JONES DAY
555 California Street, Suite 2600
San Francisco, CA 94104.1501
Telephone: +1.415.626.3939
Facsimile: +1.415.875.5700

Attorneys for Plaintiff
MICRON TECHNOLOGY, INC.

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

MICRON TECHNOLOGY, INC.,

Plaintiff,

v.

UNITED MICROELECTRONICS
CORPORATION, FUJIAN JINHUA
INTEGRATED CIRCUIT CO., LTD.,
and DOES 1-10,

Defendants.

Case No. 4:17-CV-06932-JSW

**DECLARATION OF JONATHAN S. HELLER
IN SUPPORT OF PLAINTIFF'S OPPOSITION
TO DEFENDANT UMC'S MOTION TO
DISMISS FOR LACK OF PERSONAL
JURISDICTION**

Judge: Hon. Jeffrey S. White
Courtroom: 5, 2nd Floor
Hearing: March 23, 2018 at 9:00 a.m.
Complaint Filed: December 5, 2017

DECLARATION OF JONATHAN S. HELLER

I, Jonathan S. Heller, declare as follows:

1. I am a cyber defense incident response analyst at Micron Technology, Inc. ("Micron") with my official title being Micron IT Security Analyst, Incident Response. I submit this declaration in support of Micron's Opposition to United Microelectronics Corporation's ("UMC") Motion to Dismiss for Lack of Personal Jurisdiction and in support of Micron's Opposition to UMC's Motion to Stay Discovery. In my position at Micron, I have personal knowledge of the following facts such that I could competently testify as to their truth and

1 accuracy, except as to those matters stated on information and belief.

2 2. I have served as an IT Security Analyst at Micron for two years. Additionally, I
3 have a Bachelor's of Science in Information Systems Security from the American Military
4 University, and I have over ten years' worth of work experience in the field of cyber security.

5 3. I am one of the primary investigators at Micron for anything related to cyber
6 incidents from a defensive perspective. This means that I am called on to analyze any suspicious
7 computer or digital activity that may occur. Specifically, my duties include the investigation of
8 data loss prevention and theft of Micron's proprietary and trade-secret data by departing
9 employees. I do not investigate every departing employee, but rather only those that get flagged
10 for some reason, such as was done with Kenny Wang when Micron concluded that he lied about
11 where he was going after Micron.

12 4. I was directed to conduct an investigation into Mr. Wang's emails and computer
13 activity during the weeks preceding his departure from Micron. On September 16, 2016,
14 Micron's IT department obtained Wang's laptop from the IT Director at Micron Memory Taiwan
15 ("MMT") and promptly gave it to me. On that same day, I imaged the laptop's hard drive using
16 Encase Forensic Software, a reliable software that makes an exact duplicate of a hard drive. In
17 other words, the image I took of Wang's laptop is an accurate representation of everything on the
18 laptop at the time I received it.

19 5. During my investigation of Wang's laptop, I discovered attempts by Mr. Wang to
20 cleanse his laptop, but despite efforts to erase data, I have still been able to access enough to
21 verify the theft of proprietary and trade-secret data. For example, I have been able to verify that
22 hundreds of files were uploaded to Mr. Wang's Google Drive account, as well as through the
23 USB port of his computer to either a thumb drive or other electronic device.

24 6. Recently, I was further asked to determine if any of these documents came directly
25 from a Boise, Idaho server. I have been able to verify that several documents indeed came from a
26 server in Boise, Idaho, and I expect to find many more as I manually go through each file name
27 and cross-reference it to Mr. Wang's access activity on the Boise servers.

28 7. Similarly, I have been able to collect information from Micron's Data Loss

1 Prevention (“DLP”) server to determine that 931 files were transferred to an external device
2 through the USB port of Mr. Wang’s computer during the two weeks preceding his departure.
3 Additionally, I have verified that several of these documents definitely came from the Boise
4 servers by (i) manually going through each file name one-by-one (still in process), (ii) searching
5 for the same filename on the Boise server(s), (iii) accessing the file on the Boise server and/or Mr.
6 Wang’s laptop image to determine if there exists any record of when it was accessed by any
7 Micron employee(s), and (iv) verifying whether Mr. Wang accessed it in the weeks preceding his
8 departure. Using this method, I can verify the dates and times of those files accessed by Mr.
9 Wang that correspond to the file names of documents that were transferred to his Google Drive
10 account or USB drive. While I can verify that Mr. Wang accessed these files from the Boise
11 servers, I have not yet been able to determine whether he altered those files in any way before
12 transferring them from his laptop to other media. I expect to find many more files that came from
13 the Boise servers as I continue to manually cross-reference each file name with access activity on
14 the Boise servers and/or Mr. Wang’s laptop image.

15 8. Thus far, most, if not all, of the documents I have identified contain very sensitive,
16 proprietary Micron information.

17 9. Additionally, Micron has servers in Milpitas, in Santa Clara County, California.
18 The search is ongoing to determine if any files were accessed by Mr. Wang from these servers.

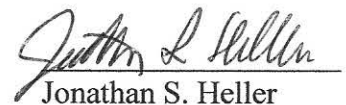
19 10. Individuals downloading files from the Boise servers should be aware that they are
20 accessing the files from the Boise location. The servers have always been located in Boise,
21 Idaho, and I believe this is commonly known within the company. The most common method for
22 accessing files from these servers is through a web-based interface called Sharepoint, which has
23 always been located on the Boise servers. Additionally, many times the URL that appears in the
24 browser window will have a designation as to the project, (such as “Fab4,” which would indicate
25 a Fabrication facility), which the user should know is located in the United States. Furthermore,
26 sometimes the URL will have the abbreviation MTI, which is short for Micron Technology, Inc.,
27 and would be associated with Micron headquarters in Boise, Idaho.

28 11. While I have been able to determine a lot from the data in Micron’s possession, the

1 best evidence still resides in the possession of Mr. Wang, UMC, and/or third parties like Google.
2 First, Micron has only been able to obtain through forensic analysis a partial list of filenames
3 uploaded by Mr. Wang. Since Micron has no way of knowing whether the list of filenames is a
4 complete list, Micron will need access to Mr. Wang's Google Drive and any portable electronic
5 devices ever owned or used by Mr. Wang and in Mr. Wang's or UMC's possession. Second,
6 access to the actual files corresponding to the partial list of filenames would provide Micron with
7 valuable metadata and a more accurate picture of the data theft. Therefore, Micron needs access
8 to Mr. Wang's Google Drive and portable electronic devices, as well as access to the actual files
9 that were stolen.

10
11 I declare under penalty of perjury under the laws of the United States and the State of
12 California that the foregoing is true and correct.

13
14 Executed this 1st day of March, 2018, at Boise, Idaho.

15
16
17 
Jonathan S. Heller

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the above and foregoing documents have been served on March 1, 2018 to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

Executed on March 1, 2018, at San Diego, California.

By: s/ Randall E. Kay

Randall E. Kay